Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/US05/000068

International filing date: 05 January 2005 (05.01.2005)

Document type: Certified copy of priority document

Document details: Country/Office: AR
Number: P040100013
Filing date: 05 January 2004 (05.01.2004)

Date of receipt at the International Bureau: 23 June 2005 (23.06.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

MS/05/68

REPÚBLICA ARGENTINA
PODER EJECUTIVO NACIONAL
MINISTERIO de ECONOMÍA y PRODUCCIÓN
SECRETARÍA de INDUSTRIA, COMERCIO y de la PEQUEÑA y MEDIANA EMPRESA
INSTITUTO NACIONAL de la PROPIEDAD INDUSTRIAL

CERTIFICADO DE DEPÓSITO

COPIA OFICIAL CONVENIO DE PARIS - LISBOA 1958 -

ACTA N° P 20040100013

LA ADMINISTRACION NACIONAL DE PATENTES, CERTIFICA QUE CON FECHA 5 DE ENERO DE 2004 SE PRESENTÓ A NOMBRE DE SALVA CALCAGNO, EDUARDO LUIS; CON DOMICILIO LEGAL EN PARAGUAY 610 PISO 17 CAPITAL FEDERAL, REPUBLICA ARGENTINA (AR).

UNA SOLICITUD DE PATENTE DE INVENCIÓN RELATIVA A: PROCEDIMIENTO Y TARJETA MULTI - CLAVE PARA EVITAR FRAUDES POR INTERNET

CUYA DESCRIPCIÓN Y DIBUJOS ADJUNTOS SON COPIA FIEL DE LA DOCUMENTACIÓN DEPOSITADA EN EL INSTITUTO NACIONAL DE LA PROPIEDAD INDUSTRIAL.

SE CERTIFICA QUE LO ANEXADO A CONTINUACIÓN EN 40 FOJAS ES COPIA FIEL DE LOS REGISTROS DE LA ADMINISTRACIÓN NACIONAL DE PATENTES DE LA REPÚBLICA ARGENTINA DE LOS DOCUMENTOS DE LA SOLICITUD DE PATENTE DE INVENCIÓN PRECEDENTEMENTE IDENTIFICADA.

A PEDIDO DEL SOLICITANTE, EXPIDO LA PRESENTE CONSTANCIA DE DEPOSITO EN BUENOS AIRES, REPUBLICA ARGENTINA, A LOS 29 DÍAS DEL MES DE DICIEMBRE DE 2004.

DR. EDUARDO ARIAS
COMISARIO
ADMINISTRACION NACIONAL DE PATENTES

Caso No. 20172

Memoria Descriptiva

de solicitud de

Patente de Invención

Relativa a:

PROCEDIMIENTO Y TARJETA MULTI-CLAVE PARA EVITAR FRAUDES POR INTERNET

A favor de:

SALVA CALCAGNO, EDUARDO LUIS

PROCEDIMIENTO Y TARJETA MULTI-CLAVE PARA EVITAR FRAUDES POR INTERNET

Campo técnico de la invención

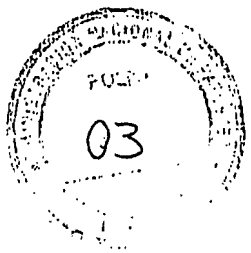
La presente invención trata sobre un procedimiento de seguridad especialmente diseñado para legitimar transacciones y evitar los fraudes por Internet, los que se cometen usualmente por medio del robo de datos sensibles, los que luego son utilizados para realizar operaciones ilícitas. También se divulga una tarjeta Multi-clave, necesaria para poner dicho procedimiento en práctica.

Antecedentes del Estado de la Técnica

Las redes de comunicaciones constituyen la clave de la transmisión de información en Internet, y también en muchos otros canales, como la telefonía móvil, etc. Cualquier sistema interconectado puede ser considerado una red. Sin embargo en el plano informático, en la actualidad se considera a Internet como la red menos segura para los usuarios.

Prueba de ello es que numerosas empresas tratan determinadas partidas de sus presupuestos como información confidencial, en especial las concernientes a seguridad de redes informáticas.

Se calcula que las empresas de todo el mundo han invertido en este año la cantidad de 6300 millones de dólares para proteger sus redes informáticas, previendo que la facturación en este campo se duplicará en los próximos 3 años hasta alcanzar los 12.900 millones.



No obstante las pocos casos por año denunciados de fraude informático en relación con la gran cantidad de delitos reales cometidos, se estima que las pérdidas ascienden a 2 dólares por cada 1000 de productos cobrados.

Vale hacer un breve repaso del funcionamiento actual de Internet para destacar sus costados débiles.

La idea básica de Internet es que dos computadoras remotas puedan establecer una comunicación entre ellas, valiéndose de un soporte físico. El par telefónico y el cable-módem son algunos de los más conocidos en la actual oferta de comunicación a través de Internet.

Además del soporte físico, existe un protocolo de comunicaciones que permite que todas las computadoras se "entiendan" entre sí a través de servidores, que son grandes CPU al servicio de una cartera de clientes a los cuales se les sirven direcciones electrónicas para correo o un espacio en la web, además de los servicios FTP o chat, por ejemplo.

Después de los servidores, están los nodos de conexión o enrutadores que facilitan los "saltos" a efectuar hasta llegar a destino. Estos enrutadores son sistemas que guían nuestros datos hacia una dirección predeterminada. Como sucede con los números de teléfono, cada página web tiene una asignación numérica como dirección electrónica (IP), siendo imprescindible para alcanzarla el rastreo de los nodos de conexión necesarios. Luego, las páginas son leídas gracias a un navegador instalado en nuestra computadora, que es capaz de marcar la dirección IP, capaz de soportar el protocolo determinado y de interpretar las respuestas del lugar IP.

El navegador puede a su vez guardar cada parte de la página descargada, modificarla o procesarla, además de enviar y recibir archivos bajo programas específicos.

Todos estos elementos son a grandes rasgos, los que actúan cuando nos conectamos a Internet, procedimiento que repetimos rutinariamente introduciendo nuestra contraseña y nuestro nombre de usuario. Estos dos datos fundamentales, son comprobados por nuestro servidor para validar nuestra conexión y acceso, los que nos dará "derecho" a realizar las operaciones que hayamos convenido de antemano con nuestro servidor.

Ahora bien, si los datos pueden viajar de un lado a otro, también es posible mantener otro tipo de operaciones, como el intercambio de archivos entre ellos. Esto se consigue mediante FTP, un estándar de comunicaciones que permite "leer" el disco rígido de otra computadora remota y bajarse todo o algo de él, con previa autorización.

Por otro lado, con FTP podemos también enviar cualquier archivo desde nuestro disco rígido hacia otro disco rígido de computadoras remotas. Y es aquí donde comienzan los problemas de seguridad en Internet, ya que de este modo se penetra al sistema y se obtienen passwords de acceso.

Hoy en día, es habitual leer en los periódicos noticias relacionadas con fraudes informáticos, producto de las actividades de hackers, crackers, lamers, copyhackers y demás integrantes de la "familia" de delincuentes electrónicos. Catalogados todos ellos como "piratas informáticos" y sin entrar a detallar la operatoria más común de cada uno de estos grupos, se pueden enumerar sin embargo, cuáles son los resultados más dañinos de su accionar, a saber:

- Robo de datos sensibles de bases de datos puestas en Internet.
- Falsificación de identidad, duplicación de identidad.
- Operaciones comerciales por Internet utilizando los datos robados.

- Duplicación de tarjetas de crédito, de débito y de otros tipos.
- Falsificación de documentos: escrituras de propiedades inmuebles, créditos, préstamos, extractos bancarios, etc.

Solo hemos detallado lo que nos concierne acerca del problema a resolver que se plantea la presente invención, que es el robo de datos sensibles de la red y su posterior utilización para operaciones comerciales fraudulentas. No es el propósito de esta invención evitar la propagación de virus o el crackeo de sistemas por Internet.

Ante la situación actual de inseguridad que ofrece la web para realizar operaciones que impliquen transacciones comerciales, han surgido ciertas respuestas por parte de las empresas informáticas: la instalación de firewalls, la encriptación de datos en sus versiones más complejas y otros tipos de defensas que no vamos a enumerar en detalle. Simplemente, se desea destacar que en todos los casos, existen dos "puntos" en el sistema: aquel desde donde se envía la información y el que la recibe y almacena, consistiendo todas las soluciones que ofrece la técnica actual en limitar al máximo o impedir el acceso a estas bases de datos que contienen información sensible con las que se podría realizar fraudes como los que se detallaron.

Todos los esfuerzos contra los piratas informáticos han sido concentrados en este sistema de dos puntos, reforzando al máximo y encriptando los datos de modo de dificultar el acceso y posterior uso de los mismos por parte del hacker. No obstante, estas soluciones no han dado el resultado esperado. Solo basta con leer a diario las noticias de estafas y fraudes millonarios cometidos en perjuicio de corporaciones multinacionales o de clientes particulares que

descubren que su tarjeta de crédito ha sido clonada y utilizada en su nombre a través de la web.

Esto sucede porque en el sistema de dos puntos utilizado actualmente, la base de datos está siempre disponible en una red accesible, sea a través de módem u on line, por lo que el hacker puede robar los datos de un punto, por ejemplo un PIN o NICK de una tarjeta de un usuario determinado y luego con esa información operar en la base de datos accesible, que reconocerá como "buenos" a esos permisos y habilitará al delincuente informático a comenzar su tarea delictiva.

Ahora bien, qué sucedería si se cambiara el sistema actual de dos puntos y se aislara uno de ellos, el que contiene los datos sensibles, de modo que no estuviera disponible en red; mientras que el otro punto, el que contiene los permisos quedara aislado como una serie de datos inconexos cuyo robo de nada serviría sin la base de datos en la cuál debieran operar?

La presente patente de invención tiene por finalidad resolver el problema planteado en el arte previo por medio de un procedimiento que modifica las etapas operatorias conocidas, aislando la base de datos de la red accesible e introduciendo una tarjeta de seguridad Multi-clave que no permite hacer dos operaciones con el mismo PIN, debido a un sistema de convalidación de los mismos.

La seguridad y salvaguarda que otorga esta tarjeta multiclave utilizada en el procedimiento reivindicado consiste en que nunca se sabe de antemano cuál será el próximo PIN o código alfanumérico que utilizará el cliente poseedor de la tarjeta multiclave para su próxima transacción.

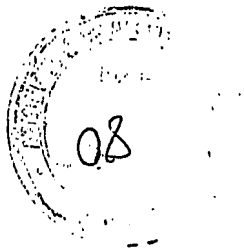
Por esa razón, los hackers no podrán hacer uso de tarjetas robadas, adulteradas o falsificadas, ya que es el propio titular quien legitima su compra, como ya se detallará más adelante, con cada PIN utilizado.
Asimismo, este procedimiento elimina la posibilidad que el usuario entregue información sensible de su tarjeta de crédito o débito, como ser el número de la cuenta misma y todos los datos que hacen a su identificación, en la red accesible, tal como se realiza en cualquier operación actualmente por Internet.
Lo único a lo que podrá acceder un delincuente informático es al último PIN utilizado, pero sin saber a qué cuenta está asociado ni cuál será el próximo PIN a usar por parte del cliente, ya que el último quedó automáticamente anulado y descartado del sistema de convalidación.

En resumen, podríamos decir que existen en la actualidad, dos tipos de identificadores utilizados para operaciones electrónicas:

Intrínsecos :Impronta ADN, Fondo de ojo, Iris, Huellas dactilares, fisonomía de las manos, Timbre de voz, cinemática de la firma manuscrita, etc.

Extrínsecos: PINS, passwords, firma manuscrita, datos históricos, números de cuentas bancarias, etc.

La seguridad de los identificadores extrínsecos, una vez utilizados, queda comprometida porque el sistema los expone al estar contenidos en bases de datos accesibles a través de la Web, por ejemplo:



Los Números PIN

- Es un caso de típico de identificador Extrínseco.
- Es el método utilizado en las tarjetas de banda magnética.
- Es un secreto compartido entre el usuario autorizado y el sistema.
- El PIN debe introducirse en el sistema antes de que la tarjeta pueda ser utilizada.
- El nivel de seguridad que proporcionan es realmente débil.
- El PIN sólo proporciona protección frente atacantes técnicamente no formados y sin recursos.
- El usuario no elige un número realmente inimaginable, sino que tiende a apuntar un número que le es fácil de recordar.
- En el caso de escenarios como Internet: al introducir el PIN se hace sobre un equipo inseguro, el mismo puede ser capturado y re-usado, haciendo totalmente vulnerable a la red y el comercio a través de la misma.

La seguridad del procedimiento propuesto se basa en una serie de componentes que combinados producen un producto seguro, novedoso e inventivo frente al estado actual de la técnica.

Dichos componentes son:

- Concepto de OTP (One Time Password), lo que significa que una vez utilizado un password no pueda volver a usarse y la captura de dicha clave no sea útil para nadie.
- Autenticación biométrica de la identidad de quien recibe la tarjeta que contiene las claves a usar (a través de la huella digital, la firma y su ADN).

- Autenticación de la identidad del usuario por el uso combinado de dos claves (NICK de usuario + PIN aleatorio), que el mismo conoce por estar impresas en su tarjeta Multi-clave, más el conocimiento de la empresa sobre la que va a realizar la transacción (este último dato es el que invalida el uso de la tarjeta ante la pérdida de la misma).

Y lo más importante,

- Total Protección de los datos sensibles de los clientes (datos personales, cuentas bancarias, saldos, etc.) por estar en una base de datos fuera de la red.

Breve descripción de las figuras

La figura 1 muestra el diagrama de flujo de la fase inicial de fidelización de una empresa X para operar con el Centro de Autorizaciones.

La figura 2 consiste en la etapa de ingreso y actualización de datos de los usuarios de la empresa X.

La figura 3 muestra el proceso de solicitud y entrega de tarjetas Multi-clave a la empresa X por parte del Centro de Autorizaciones y de la Empresa X a sus usuarios.

La figura 4 detalla el proceso de generación de tarjetas Multi-clave.

La figura 5 muestra el diagrama de flujo de la autenticación de identidad a través de una página Web.

La figura 6 muestra el diagrama de flujo de la autenticación de identidad a través de un Call Center.

La figura 7 muestra el accionar posterior del usuario, una vez que ha sido legitimada su identidad.

La figura 8 muestra la configuración de la tarjeta Multi-clave utilizada en el procedimiento propuesto.

Descripción detallada de la invención

El procedimiento propuesto se lleva a cabo a través de una tarjeta Multi-clave que se entrega al usuario, con la cuál este podrá realizar las operaciones por Internet que crea convenientes.

Esta tarjeta (Figura 8) plástica y flexible, del tamaño habitual que tienen las tarjetas magnéticas, tiene varias particularidades que la diferencian de las tarjetas conocidas: no tiene los datos personales del usuario, ni el nombre, ni su dirección ni identificación alguna de la empresa a la que pertenece o con la cuál se puede operar con dicha tarjeta.

En el contrafrente de la misma, posee impreso el NICK del usuario que viene oculto por una capa protectora tipo Scratch-off (raspadita). También se prevé un modo de realización alternativo en el cuál el NICK viene impreso sobre una tira plástica opaca removible, de modo que el usuario la retire y la pueda pegar, por ejemplo en el frente de la PC de su casa, desde la cuál operará con su tarjeta Multi-clave.

En el cuerpo central de la tarjeta, posee impresos una serie variable de PINS (códigos alfanuméricos), cuyo modelo standard es de 30 a 50 PINS variando la impresión de PINS según la utilidad que se le dé a la tarjeta Multi-clave, pudiendo existir modelos especiales de dichas tarjetas. Estos PINS están todos ocultos por una capa protectora tipo Scratch-off (raspadita), que el usuario irá

descubriendo a medida que los vaya utilizando, quedando los PINS descubiertos y dados a conocer, inhabilitados para una próxima operación.

Los otros datos que incluye la tarjeta Multi-clave son el código identificador único de partida, emitido por la imprenta del Centro de Autorización al momento de generar una partida determinada de tarjetas para una empresa X, y un código identificador de tarjeta consistente en un código único alfanumérico de X (standard 10) caracteres, que identifica a esa tarjeta Multi-clave, relacionándola con el usuario y con los PINS autorizados para usar.

El frente de la tarjeta podrá contener espacio para publicidad y otros datos menos relevantes, por ejemplo la fecha de expedición de la misma y vencimiento.

La tarjeta Multi-clave viene envuelta en un celofán termosellado, evitando roces o raspaduras que puedan dejar al descubierto los códigos ocultos de NICK + PINS.

Como se podrá advertir, otra norma de seguridad adicional que provee el procedimiento reivindicado, además de un proceso de identificación del usuario por huella dactilar que se describirá más adelante, reside en el hecho que la tarjeta no tiene datos identificatorios que pudieran ser de utilidad a un eventual ladrón que pudiera haberle robado la tarjeta al usuario. No hay forma de relacionar esa tarjeta con el usuario ni con la empresa X que se la entregó, ya que toda esa información se halla contenida en la base de datos no accesible en la Web, razón por la cuál la tarjeta robada será de nula utilidad para otro que no sea su titular legítimo.

Para revelar el procedimiento que se desea proteger, es necesario en primera instancia describir las distintas entidades que intervienen en el mismo.

- **Empresa X:** Es la entidad que realiza los Servicios de Banca Electrónica, Sistemas de Pago y-o Comercio Electrónico, entre otros servicios. Dichos servicios los brinda a través de Internet y/o de un Call Center, necesitando dar seguridad a sus usuarios.

- **Usuario :** es el individuo que desea utilizar los servicios brindados por la empresa X a través de Internet o de un Call Center.

- **Centro de Autorizaciones (CA):** Es la entidad que brinda el servicio a la empresa X de autorizar al usuario para que pueda utilizar de manera segura los servicios brindados. El Centro de Autorizaciones es el que lleva a cabo los procedimientos de generación de tarjetas, asignación de alias o NICKS a los usuarios y habilitación de las tarjetas para su uso.

- **Call Center:** Es la entidad que brinda el servicio de autorización de los usuarios de la empresa X a través de un llamado telefónico. (Está dentro del Centro de Autorizaciones, es parte de él).

Descripción de los Procedimientos o Fases:

- **Fase 1 (Figura 1) - Fidelización de Empresa X para operar con el Centro de Autorizaciones (CA)**

La Empresa X decide adherirse al sistema de seguridad que utiliza el procedimiento reivindicado y se pone en contacto con el Centro de Autorizaciones a los efectos de firmar un convenio de adhesión.

El Centro de Autorizaciones ingresa en su base de datos aislada y desconectada no disponible en la Web, los datos de la empresa asignándole a la misma un código identificatorio único. A partir de este momento la Empresa X deberá enviar la información de los usuarios que harán uso del sistema de seguridad.

- **Fase 2 (Figura 2): Ingreso y actualización de datos de los usuarios de la Empresa X**

La Empresa X envía la información de los nuevos usuarios que van a hacer uso del sistema. En esta fase también se considera el caso de la notificación de las modificaciones o bajas de usuarios que se produzcan cuando la empresa este operando con el sistema.

A partir de la recepción de novedades de usuarios el Centro de Autorizaciones elabora el registro NICK de usuarios de la Empresa X asignándole a cada usuario un alias o NICK que lo identifica unívocamente y resguarda su identidad. El Centro de Autorizaciones actualiza su Base de Datos ingresando los usuarios nuevos con el NICK asociado a cada uno y actualizando o dando de baja los usuarios que corresponda según lo informado por la Empresa X.

Hasta aquí, ningún dato está disponible en Internet, puesto que la base de datos con los NICKS asignados no está disponible en red y si la empresa X hubiera enviado la lista de usuarios por Internet y no por correo o CD-Rom, esta información carecería de valor, puesto que se trataría de un listado de personas sin asociación a cuenta alguna.

14

- **Fase 3: Solicitud de Tarjetas Multi-clave de Empresa X y posterior generación de dichas Tarjetas Multi-clave.**

3.1 (Figura 3): Solicitud de Tarjetas Multi-clave de Empresa X

La Empresa X solicita al Centro de Autorizaciones las tarjetas Multi-clave para sus usuarios a través de una Nota de Pedido. El Centro de Autorizaciones genera una partida de tarjetas que entrega a la Empresa X para que la distribuya en forma personalizada. El usuario recibe la tarjeta y debe autenticar su identidad a través su firma y de un sello de seguridad orgánico divulgado en la solicitud de patente en trámite P 00 01 05051 del mismo solicitante, que aquí se incorpora como referencia.

Este sello de seguridad, comercializado bajo la marca DigiFirma ®, consiste en un soporte capaz de guardar la huella dactilar y el ADN de la persona ingresada, extraído de sus huellas digitales por medio de reactivos y lecturas microscópicas que pueden levantar restos orgánicos de células pegadas en el adhesivo del sello de seguridad orgánico.

Este sello es de vital importancia para evitar un tipo de fraude muy común en la actualidad: el de sustitución de personalidad.

Con los sistemas actuales de distribución, un delincuente puede fácilmente con un documento falsificado, hacerse pasar por otra persona y de este modo obtener, por ejemplo, una tarjeta Multi-clave como la que se divulga en la presente patente de invención. El falsificador recibirá por correo su tarjeta y firmará en el recibo de correo con una firma falsa, al igual que su identidad, tras lo cuál podrá cometer todo tipo de fraudes hasta que los mismos sean detectados por la persona cuya identidad fue robada. Ya a esta altura, la tarjeta

habrá sido usada hasta sus últimas consecuencias y los daños serán irreparables.

En el procedimiento propuesto y gracias al mencionado sello de seguridad, la Empresa X ha solicitado previamente a través de una nota de pedido, las tarjetas Multi-clave para una lista de usuarios determinados; tras lo cuál en Centro de Autorización generará una partida de tarjetas que entregará a la Empresa X para que las distribuya en forma personalizada. Esta entrega se realiza a través de un formulario especial que cuenta con el mencionado sello de seguridad orgánico, de modo que el usuario deba dejar obligatoriamente su huella dactilar y su ADN en dicho sello, que remitido nuevamente al Centro de Autorizaciones será cargado en la Base de Datos, relacionando identidad, huellas dactilares, NICK, código identificador de tarjeta, PINS para usar y demás datos filiatorios del usuario.

De esta manera, se suman medidas de seguridad que hacen al procedimiento propuesto mucho más efectivo que los sistemas conocidos en la actualidad, evitando ya al inicio del procedimiento un posible fraude por falsificación de personalidad, puesto que si algún usuario quisiera realizar algún tipo de delito con la tarjeta Multi-clave, será inmediatamente identificado puesto que tuvo obligatoriamente que dejar su huella en el formulario al momento de recibir la tarjeta Multi-clave.

Una vez realizada la distribución de las tarjetas, la Empresa X le informa al CA para que habilite en la Base de Datos los NICK de los usuarios que han recibido la tarjeta Multi-clave, de modo que dichos usuarios puedan hacer uso de las tarjetas.

3.2 (Figura 4) : Generación de Tarjetas Multi-clave.

El Centro de Autorizaciones genera las tarjetas en partidas asignándole a cada una un código de tarjeta único alfanumérico de X caracteres (números, letras mayúsculas y/o letras minúsculas), un NICK de usuario y una cantidad de PINS a definir. El proceso de generación verifica que un PIN no se repita en una misma tarjeta.

- **Fase 4: Autenticación de Identidad**

Es la fase en que el usuario con su tarjeta Multi-clave utiliza los servicios de Banca Electrónica, Sistemas de Pago o Comercio Electrónico y demás servicios ofrecidos por Internet. Para ello, tiene dos caminos: ya sea ingresando a la página Web de la Empresa X o a través de un llamado telefónico al Call Center. A continuación se detallan ambas posibilidades.

4.1 (Figura 5): Autenticación de Identidad a través de la Página Web

El usuario ingresa a la Página Web de la Empresa X y solicita su legitimación ingresando, mediante un link, al portal del Centro de Autorización.

En esta instancia, el servidor Web del CA solicita al usuario que ingrese su NICK + un código PIN elegido al azar haciendo Scratch-off en su tarjeta Multi-clave. Dichos PINS tienen temporalidad, esto significa que al ingresar el código PIN alfanumérico, el usuario tiene un tiempo limitado para realizar la operación en cuestión. Esta es una medida más de seguridad que tiende a proteger al sistema, restringiendo los grados de libertad de un posible delincuente informático.

Adicionalmente, los PINS ingresados pueden tener diferentes colores según la categoría del usuario de la Empresa X, lo que agrega un elemento más a controlar en el proceso de autenticación de identidad que se describirá a continuación.

Una vez ingresados los códigos NICK + PIN, dicho servidor Web del CA traduce la cadena alfanumérica en códigos de barras, dentro de la nomenclatura EAN y envía este código al servidor sin conexión abierta, donde se halla la base de datos del Centro de autorización.

A partir de este momento, toda la operatoria de verificación se hará sin conexión abierta, por lo que la única información que viajó por la web que pueda ser interceptada es un código de barras aislado, de inútil uso por parte de delincuentes informáticos.

Una vez transferidos los datos a través del código de barras, el Servidor Web imprime en un rollo de obleas (A) el código de barras con información de NICK + PIN y un lector láser conectado a la base de datos del Centro de Autorizaciones lee el código de barras y verifica que el NICK esté habilitado, que el PIN corresponda al NICK y que dicho PIN no haya sido usado. Luego de este proceso de verificación, la impresión de los códigos de barras en el rollo de obleas (A) queda como constancia de las transacciones, la que oficiará de resumen mensual para la empresa X y/o del CA, donde se detallarán todas las operaciones realizadas, por qué usuarios y qué PINS han utilizado, día y hora y otros datos administrativos.

Esta verificación la realiza accediendo a la base de datos que está desconectada de la red abierta (a través de un proceso de lectura láser de los

códigos de barras con los datos a validar), impidiendo de esta manera el acceso a esta información valiosa a través de la red.
Cabe destacar nuevamente que este es el punto novedoso del procedimiento propuesto, puesto que toda la operatoria de los sistemas actuales es siempre a dos puntos, estando ambos siempre conectados a la Web, pudiendo el delincuente informático desencriptar y robar información de ambos puntos, con lo que podrá realizar los fraudes que aquí se pretenden evitar. En este procedimiento, uno de los puntos está desconectado y el otro es una serie de datos inconexos sin relación a cuenta alguna ni a ningún usuario identificable.

Una vez realizada la verificación da respuesta a la solicitud de legitimación de identidad utilizando el mismo proceso anterior pero a la inversa, el CA imprime en otro rollo de obleas (B) el código de barras de ese NICK + PIN con la autorización o negación de la transacción. A esta respuesta la lee el lector láser conectado al Servidor Web del CA y devuelve la respuesta traducida en forma instantánea y a esa combinación de NICK + PIN se la invalida en la base de datos aislada y desconectada del CA para una próxima operación. Estas obleas impresas en forma de rollos, tanto la (A) como la (B) sirven como constancia física de las transacciones realizadas y guardadas administrativamente por el CA para las empresas fidelizadas que así lo soliciten.

4.2 (Figura 6): Autenticación de Identidad a través de un Call Center

El usuario de la Empresa X desea operar con la misma y ésta solicita su legitimación mediante un llamado telefónico al Call Center.

En esta instancia el operador del Call Center solicita el NICK del usuario + un código PIN de su tarjeta Multi-clave y lo ingresa en la pantalla del sistema que dispone para la verificación de dichos datos. El sistema verifica que el NICK esté habilitado, que el PIN corresponda al NICK y que dicho PIN no haya sido usado. Una vez realizada la verificación da respuesta a la solicitud de legitimación de identidad e invalida el uso de la combinación NICK + PIN para una próxima operación.

Esta verificación se realiza accediendo a la base de datos que está desconectada de la red abierta (a través de un llamado telefónico a un Call Center), impidiendo de esta manera el acceso a esta información a través de la red. Una vez realizada la verificación da respuesta a la solicitud de legitimación de identidad.

- **Fase 5 (Figura 7): Inicio de las operaciones por Internet**

Una vez que la identidad del usuario ha sido legitimada, el mismo se encuentra en condiciones de realizar todo tipo de operaciones o transacciones comerciales, para lo cuál ingresará los datos solicitados por la Empresa X en su Página Web o vía telefónica, en caso de usar el servicio de un Call Center. La empresa X procesará la información recibida por parte del usuario, dependiendo del tipo de transacción que desee realizar, por ejemplo operaciones de E-Cash, E-Commerce mayorista o minorista, Home-Banking, legitimación de medicamentos entre laboratorios y farmacias y consumidor, Call-Center: toda operación comercial directa o indirecta para autenticación de un titular de tarjeta de compra, crédito, débito, social de salud, de seguros, etc. de las llamadas tradicionales, Para operaciones en Shoppings, Hipermercados,

etc., Hosting de Seguridad (Servidores), Para reemplazo de todo tipo de password (ej. Pin_Mail), Para control de accesos a áreas restringidas, Para autenticación de exámenes de estudiantes universitarios (ej. tarjeta Multi-clave vinculada a la PC de Bedelía), Para reemplazo del Pin fijo en Cajeros Automáticos para retiro de dinero u otras operaciones similares, Para control de diversas operaciones con la DGI, Para control de envío de remesas de dinero en forma física para dar anonimato a los exámenes clínicos de ADN y/o SIDA u otros solicitados previamente, Etc.

Ya descripto completamente el procedimiento de seguridad propuesto con el detalle de cada una de sus etapas operativas, queda en claro que la presente invención **no** es una mera actividad económico-comercial de carácter teórico, sino un procedimiento que presenta una serie de etapas (acciones) no evidentes para una persona del oficio de nivel medio, tendientes a resolver un problema planteado en el estado de la técnica basado en una combinación de elementos como ser software, hardware y la tarjeta Multi-clave con la cuál se lleva adelante toda la operatoria.

Se brindará a continuación información técnica más completa acerca de cómo se llevará a cabo la invención.

La clave del procedimiento reivindicado reside en que se apoya en un proveedor de Internet que maneja su red propia no interconectada como las demás, con su propio rango de direcciones IP, gestionando sus propios enrutadores con el protocolo BGP4. Este protocolo BGP (Border Gateway Protocol) permite conectar la red de servidores propios a múltiples operadores por dos líneas físicas STM-1 de fibra óptica (155 Mbps cada una de ellas), por

las cuáles circularán caudales de múltiples operadores con un alto rendimiento.

Como ya se dijo, la base de datos es independiente y separada de la red troncal madre de Internet a través de una conectividad láser que se produce a medida que ingresan los PINS convertidos por medio de un software en códigos de barras, los que son leídos por lectores ópticos que ubican en forma automática la clave de autorización para continuar con la transacción y certificar la misma. Dichos lectores pueden enrutar más de 40 millones de paquetes por segundo en forma automática.

Además, dicha red interna está completamente interconectada por switches (no hay hubs), los cuáles son capaces de manejar en total un ancho de barra superior a 180 Gbps.

Un dato muy importante a tener en cuenta es que este proveedor es del tipo Multihomed, con su propio Data Center; mientras que en la actualidad las empresas que ofrecen dominios, hostings y alojamiento de servidores carecen de seguridad por los siguientes motivos:

- En el caso de los operadores de telecomunicaciones, los mismos no ofrecen sus propios productos de hosting de seguridad y alojamiento en sus centros de datos. Esto trae el inconveniente que si se contrata estos servicios, el sitio web del cliente enlazará con Internet a través de una única vía, la de su operador.
- Estos proveedores son desde el punto de vista de la conectividad, meros apéndices del operador de telecomunicaciones que les da el servicio; de modo que si la línea de conexión entre el proveedor y su operador sufre un corte dejará sin servicio a todos sus clientes.

En el caso del procedimiento propuesto, el proveedor Multihomed evita esta dependencia contratando ancho de banda con distintos proveedores, valorando la conectividad de cada uno de ellos. De este modo, cada usuario conectado a Internet tiene múltiples vías de llegar a los sitios Webs alojados en el mismo y los sistemas de enrutamiento de Internet siempre elegirán la más corta de ellas, de modo que se obtienen las siguientes ventajas:

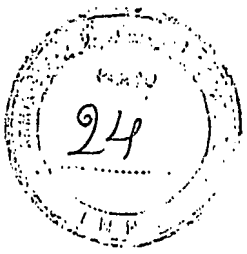
- Redundancia física: si una línea sufre un corte, las restantes mantendrán la conectividad con Internet.
- Velocidad de descarga hacia cualquier destino: los paquetes de datos escogerán la ruta más adecuada para llegar al usuario que está viendo las páginas por el camino más corto.
- Seguridad al usuario al no tener que entregar sus datos personales ni información confidencial alguna para realizar una transacción por Internet.
- Seguridad al usuario al estar protegida su identidad, N° de tarjeta de crédito y demás datos sensibles, como su capacidad crediticia y otros informes personales.
- La implementación del procedimiento propuesto redundará sin dudas en una mayor confianza en la Web para operar en la misma.

Con respecto a los sistemas operativos, el cliente puede elegir el sistema operativo que prefieran para cada uno de los planes de hostings de seguridad, ellos son Linux y Windows 2000 Server.

Los servidores basados en Linux utilizan el servidor Web Apache y disponen de la posibilidad de ejecutar scripts en Perl, Pitón y PHP4, además de acceder a bases de datos MySQL.

Los servidores en Windows incorporan el servidor Internet Information Server y pueden alojar sitios webs dinámicos utilizando páginas ASP en Visual Basic Script con acceso a bases de datos Access o SQL Server.
El hardware utilizado para ambos tipos de servidores es el IBM X330.

En resumen, el procedimiento que se reivindica reúne los requisitos de patentabilidad necesarios, además de no estar comprendido en las excepciones de patentabilidad determinadas por la Ley de Patentes, ya que se trata de una serie de etapas necesarias y consecutivas para arribar a un resultado final de resultado imprevisible (no obvio) para una persona del oficio de nivel medio.
El software provisto no se reivindica *"per se"*, sino que forma parte de un conjunto de elementos que proveen un "efecto técnico" deseado, necesario para arribar al resultado final antes mencionado y que interactúa con el hardware especificado, razón por la cuál se la considera una invención patentable.
Es evidente que podrán introducirse diversas modificaciones operativas en el procedimiento descripto, así como también en el diseño y configuración de la tarjeta, sin apartarse por ello de la esfera de la presente patente de invención que se halla claramente determinada por el alcance de las cláusulas reivindicatorias que siguen a continuación.



REIVINDICACIONES

1) Procedimiento para evitar fraudes por Internet que se realiza por medio de una tarjeta Multi-clave en el que intervienen una Empresa X, un Usuario y un Centro de Autorizaciones, caracterizado por que comprende las siguientes etapas:

Solicitar la fidelización de la Empresa X para operar con el Centro de Autorizaciones;

Dar de alta en una base de datos de dicho Centro de Autorizaciones a la Empresa X, asignándole un código identificatorio;

Enviar el registro de futuros usuarios de la Empresa X al Centro de Autorizaciones;

Elaborar un registro de NICKS de los nuevos usuarios de la Empresa X y cargarlos en la base de datos propia no disponible en la Web, constituyendo este paso dar el alta al registro de nuevos usuarios;

Solicitar mediante una orden de pedido una determinada cantidad de tarjetas Multi-clave para los usuarios habilitados a operar;

Generar en el C.A. una partida de determinadas cantidad de tarjetas Multi-clave, asignando un número único a cada partida y otro número único a cada tarjeta, relacionando este código de tarjeta con el NICK de usuario;

Distribuir dichas tarjetas Multi-clave a los usuarios correspondientes en forma personalizada, por medio de un formulario que posee un sello de seguridad orgánico donde el usuario deberá firmar y dejar su huella dactilar;

Actualizar la información de entrega de tarjetas y retornar esta información mediante los formularios de seguridad al C.A.;

Habilitar en la base de datos los NICKS de los usuarios que han recibido la tarjeta Multi-clave, actualizando de este modo las tarjetas habilitadas;

Confirmación de la habilitación a los usuarios fidelizados.

2) Procedimiento para evitar fraudes por Internet, de acuerdo a la reivindicación 1, caracterizado porque la etapa siguiente consiste en la autenticación de identidad del usuario a través de una página Web y comprende los siguientes pasos:

Ingresar a la página Web oficial de la Empresa X fidelizada, solicitando el ingreso al portal del Centro de Autorizaciones mediante un link y una vez allí ingresar el NICK + un código PIN de su tarjeta Multi-clave;

El servidor Web del C.A. imprime el NICK + el PIN ingresados, lo traduce a un código de barras, lo imprime y lo envía a la base de datos del C.A. sin conexión abierta donde un lector láser conectado a la misma lee los datos impresos anteriormente y verifica si el NICK está autorizado, si el PIN ingresado pertenece a ese NICK y si ese PIN ingresado no está anulado, autorizando la operación si las 3 verificaciones son positivas o denegando la misma si alguna de dichas 3 verificaciones da negativa;

Dicho servidor sin conexión abierta imprime el resultado de la verificación y lo envía al servidor Web, donde otro lector láser conectado al mismo lee el resultado de la verificación, autorizando o denegando la operación requerida por el usuario.

3) Procedimiento para evitar fraudes por Internet, de acuerdo a la reivindicación 1, caracterizado porque la etapa siguiente consiste en la autenticación de identidad del usuario a través de un Call Center y comprende los siguientes pasos:

Solicitar la legitimación como usuario de la Empresa X, mediante un llamado telefónico a un Call Center,

A instancias del operador del Call Center, informar el NICK de usuario + un código PIN de la tarjeta Multi-clave, datos que serán ingresados por el operador en el sistema que dispone para la verificación de dichos datos,

El sistema verifica que el NICK esté habilitado, que el PIN corresponda al NICK y que dicho PIN no haya sido usado, autorizando la operación si las 3 verificaciones son positivas o denegando la misma si alguna de dichas 3 verificaciones da negativa;

Una vez realizada la verificación, dar respuesta a la solicitud de legitimación de identidad al usuario que la solicitó telefónicamente e invalidar el uso de la combinación NICK + PIN para una próxima operación.

4) Procedimiento de acuerdo con la reivindicación 2, caracterizado por que el PIN ingresado por el usuario tiene una validez temporal limitada.

5) Procedimiento de acuerdo con la reivindicación 2, caracterizado por que el PIN ingresado por el usuario tiene un color determinado en función de la categoría del usuario poseedor de la tarjeta.

6) Procedimiento de acuerdo con la reivindicación 1, caracterizado por que el paso de generar las tarjetas Multi-clave comprende las etapas adicionales de:

Generar las tarjetas en partidas asignándole a cada una un código de tarjeta único alfanumérico de X caracteres (números, letras mayúsculas y/o letras minúsculas), verificando el sistema que no haya un código igual en la base de datos aislada no disponible en la red;

Generar un código aleatorio alfanumérico de longitud variable que será utilizado como PIN;

Repetir la operación tantas veces como PINS contenga la tarjeta Multi-clave, verificando el sistema que un PIN no se repita en una misma tarjeta;

Asignar el NICK del usuario al código de la tarjeta Multi-clave y guardar la información en la Base de Datos del Centro de Autorizaciones, dándole de esta manera el alta a esta tarjeta Multi-clave.

7) Tarjeta Multi-clave para evitar fraudes por Internet para usarse de acuerdo con el procedimiento de la reivindicación 1, caracterizada porque siendo del tamaño habitual que tienen las tarjetas magnéticas, posee impresos el NICK del usuario, una serie variable de PINS (códigos alfanuméricos) ocultos por una capa protectora tipo Scratch-off, un código identificador único de partida, emitido por la imprenta del Centro de Autorización al momento de generar una partida determinada de tarjetas para una empresa X, y un código identificador de tarjeta consistente en un código único alfanumérico de X caracteres que identifica a esa tarjeta Multi-clave, relacionándola con el usuario y con los PINS autorizados para usar; asimismo el frente de la tarjeta podrá contener espacio para publicidad.

FOLIO 28

MESA DE ENTRADAS FOLIO 20 I.N.P.I.

8) Tarjeta Multi-clave, de acuerdo con la reivindicación 7, caracterizada porque el NICK viene impreso sobre la tarjeta Multi-clave y oculto por una capa protectora tipo Scratch-off.

9) Tarjeta Multi-clave, de acuerdo con la reivindicación 7, caracterizada porque el NICK viene impreso sobre una tira plástica opaca removible.

10) Tarjeta Multi-clave, de acuerdo con las reivindicaciones 7 a 9, caracterizada porque la misma está envuelta en un celofán termosellado.

BUENOS AIRES, ENERO 2004

OBLIGADO S.C.I.A. EDA. S.A.
FEDERICO A. AULMANN
M - 1200

RESUMEN

Procedimiento de seguridad especialmente diseñado para legitimar transacciones y evitar los fraudes por Internet, que se pone en práctica con el uso de una tarjeta Multi-clave que contiene un código de identificación de tarjeta, un NICK del usuario y un número variable de PINS ocultos que sirven para realizar solo una operación, quedando luego de la misma invalidados.

El procedimiento contempla la posibilidad de que el usuario use la tarjeta Multi-clave a través de la Web o por medio de un Call Center, en ambos casos a la espera de la autenticación de su identidad por parte de un Centro de Autorizaciones. Este Centro posee una base de datos aislada y no disponible en Internet donde se guardan todos los datos sensibles que deben permanecer a resguardo para evitar cualquier tipo de falsificación. De este modo, tanto el sistema para operar por la Web como el operador del Call Center chequearán la información suministrada por el usuario (código de tarjeta + NICK + PIN) en la base de datos aislada y a continuación autorizarán o denegarán la operación, de acuerdo con el resultado del proceso de autenticación de identidad.

Figura 1

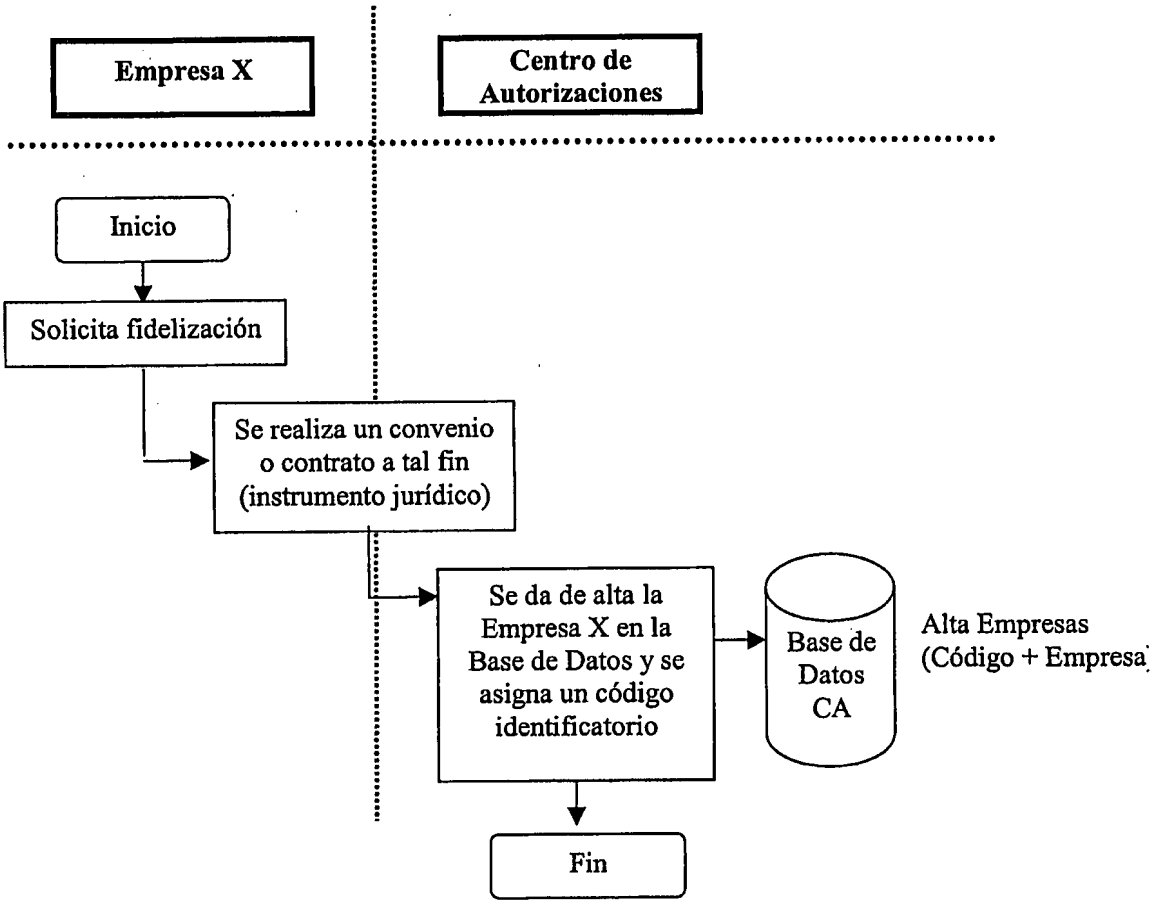

Empresa X
Centro de Autorizaciones
Inicio
Solicita fidelización
Se realiza un convenio o contrato a tal fin (instrumento jurídico)
Se da de alta la Empresa X en la Base de Datos y se asigna un código identificatorio
Base de Datos CA
Alta Empresas (Código + Empresa
Fin

Figura 2

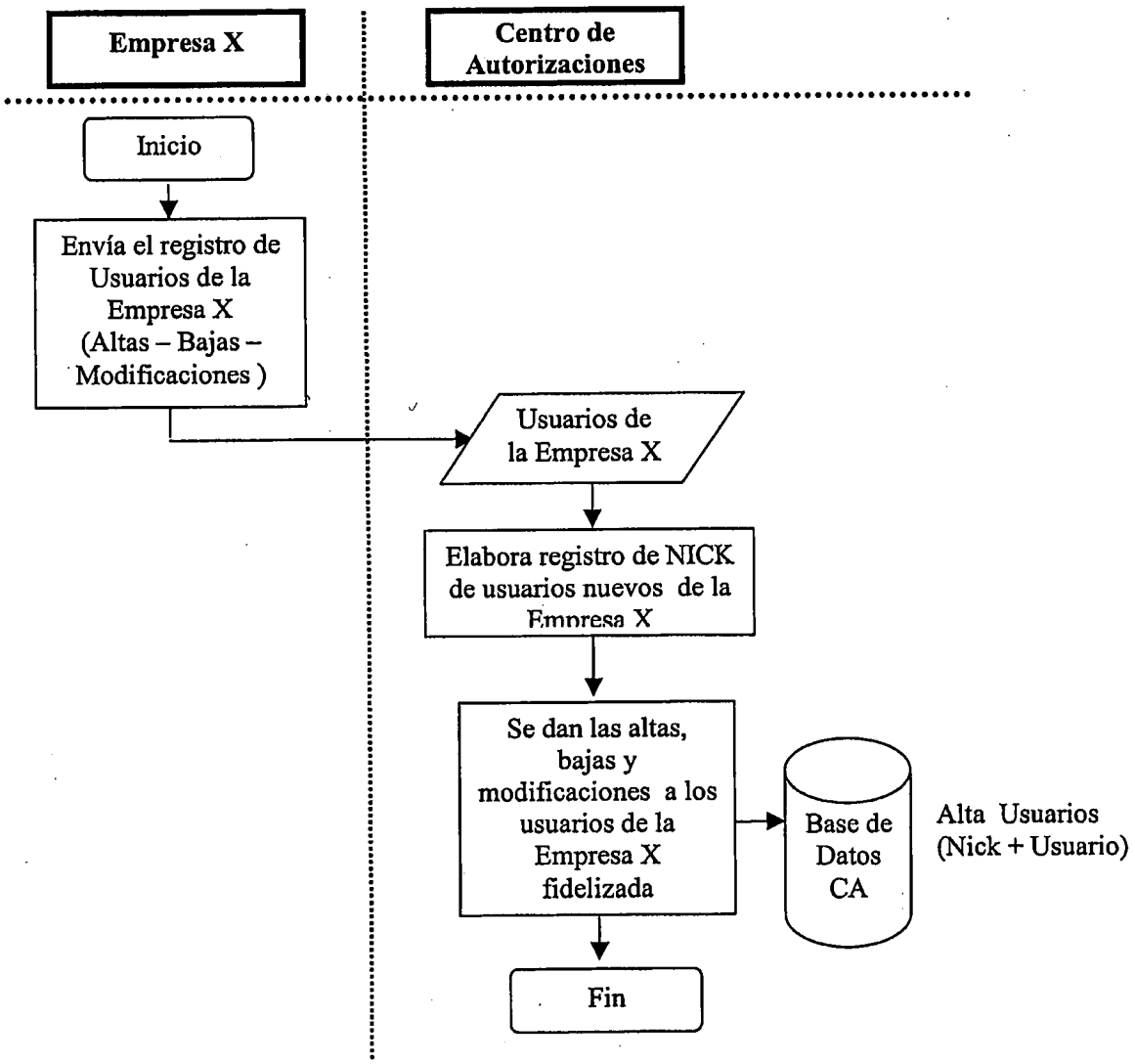
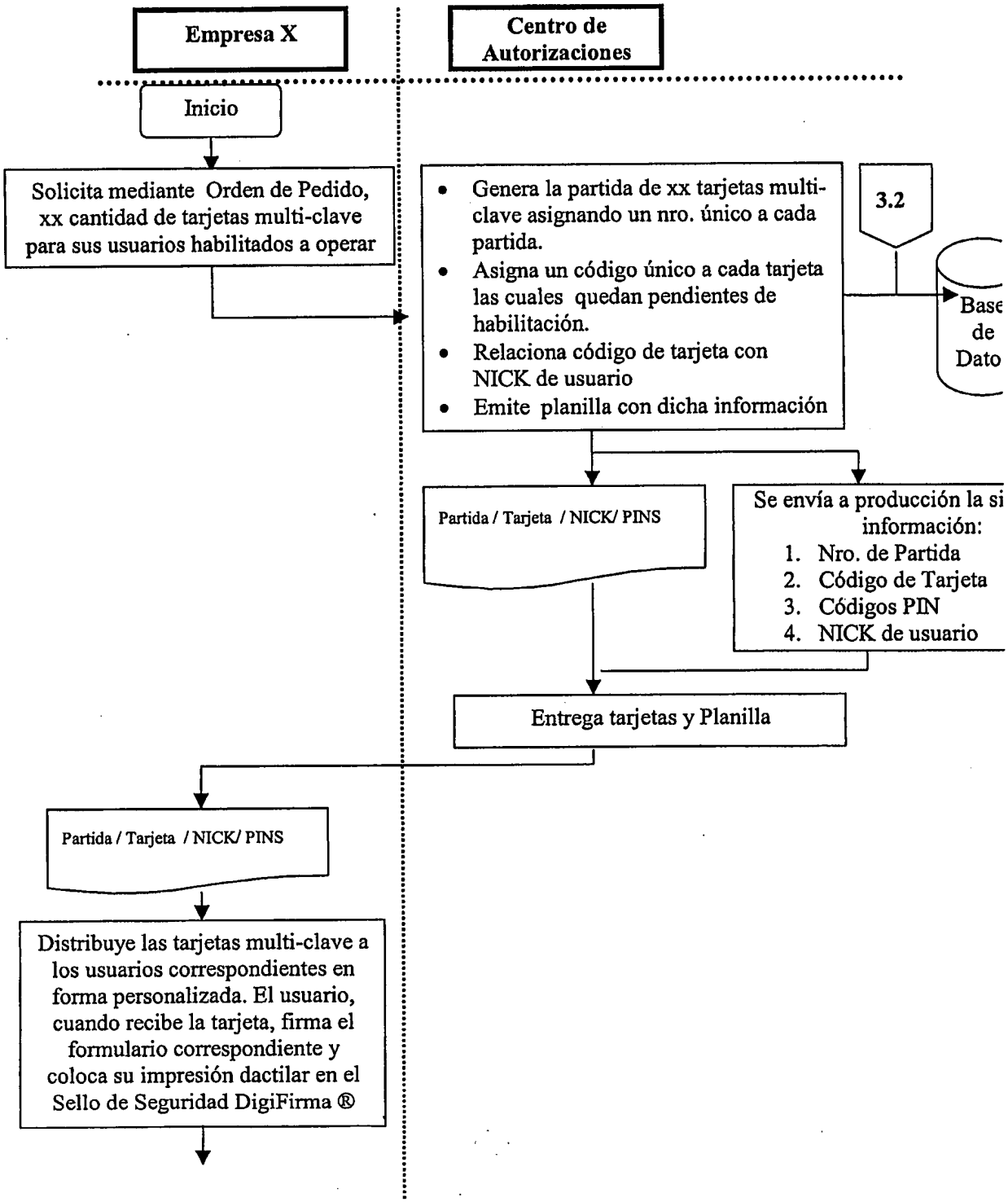


Figura 3



FOLIO
33

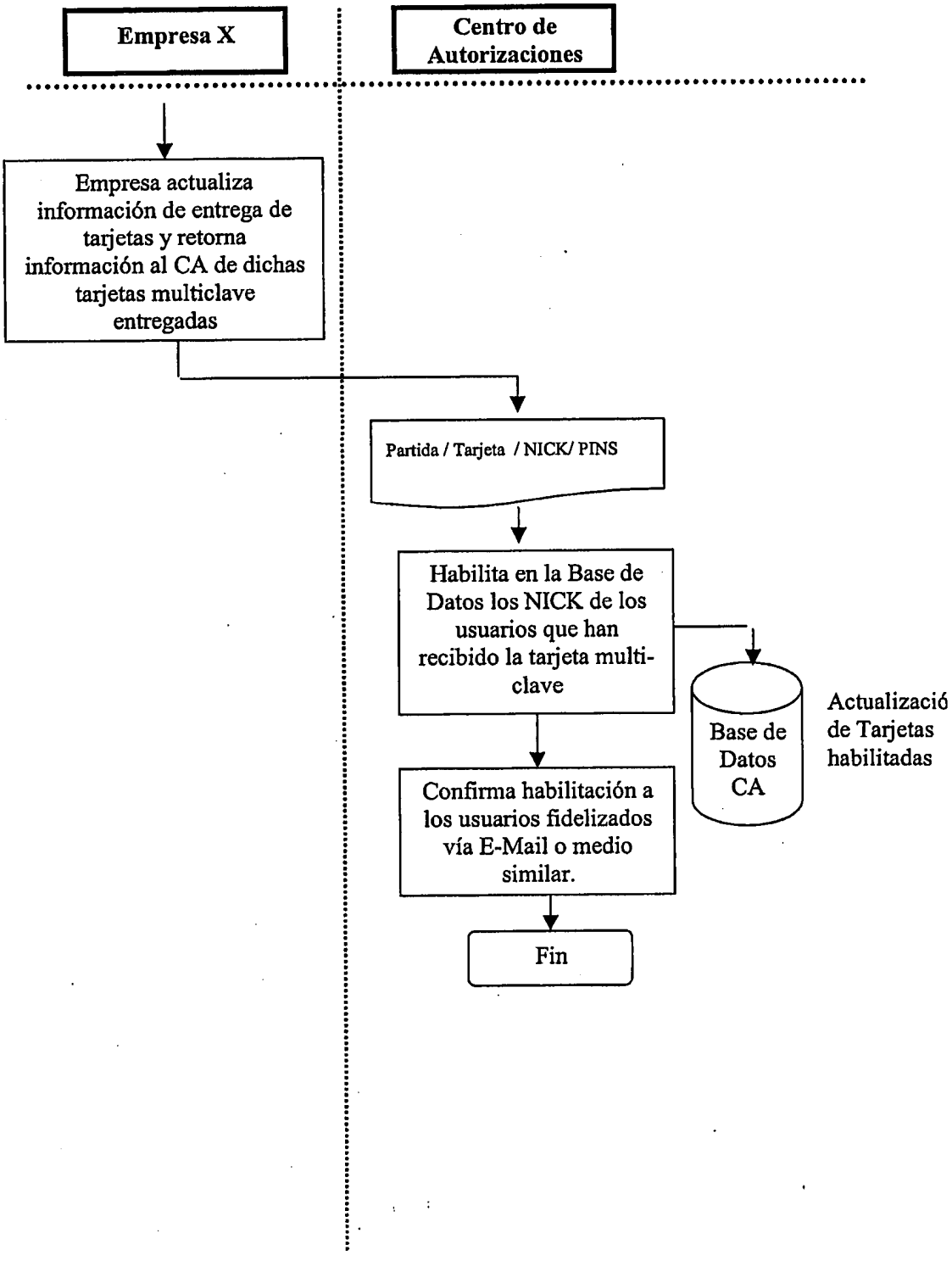
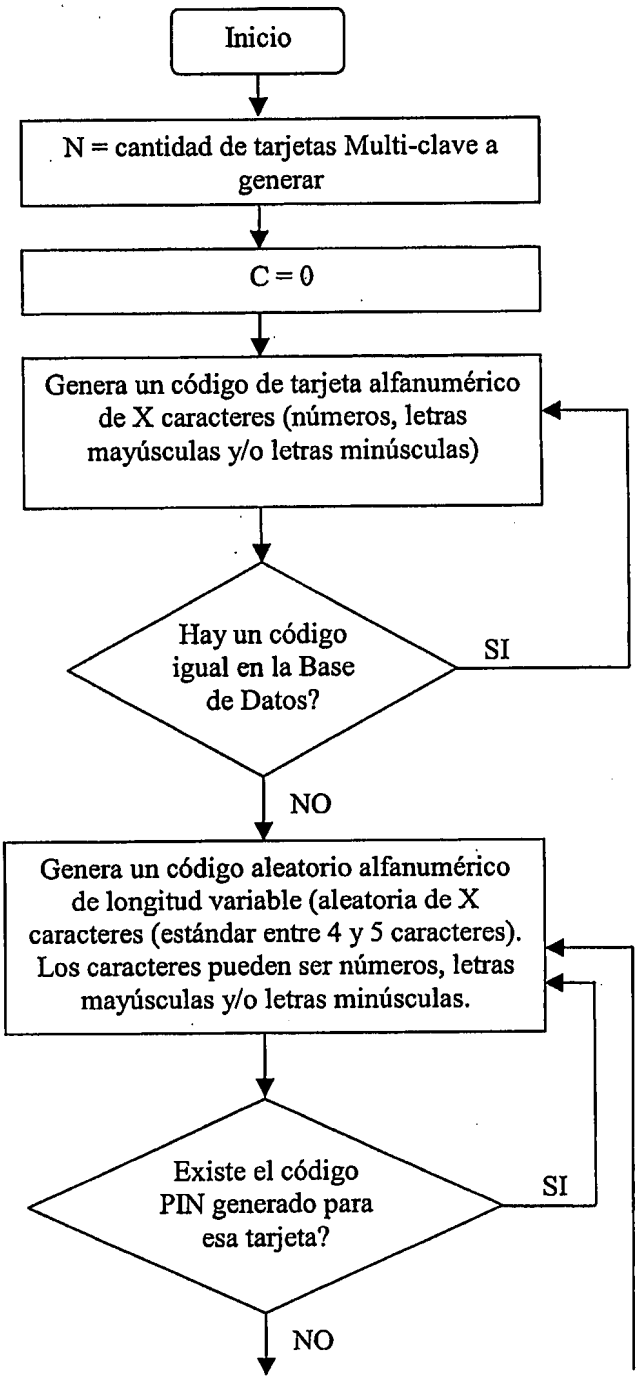

Empresa X
Centro de Autorizaciones
Empresa actualiza información de entrega de tarjetas y retorna información al CA de dichas tarjetas multiclave entregadas
Partida / Tarjeta / NICK/ PINS
Habilita en la Base de Datos los NICK de los usuarios que han recibido la tarjeta multi-clave
Base de Datos CA
Actualizació de Tarjetas habilitadas
Confirma habilitación a los usuarios fidelizados vía E-Mail o medio similar.
Fin

Figura 4


Inicio
N = cantidad de tarjetas Multi-clave a generar
C = 0
Genera un código de tarjeta alfanumérico de X caracteres (números, letras mayúsculas y/o letras minúsculas)
Hay un código igual en la Base de Datos?
SI
NO
Genera un código aleatorio alfanumérico de longitud variable (aleatoria de X caracteres (estándar entre 4 y 5 caracteres). Los caracteres pueden ser números, letras mayúsculas y/o letras minúsculas.
Existe el código PIN generado para esa tarjeta?
SI
NO

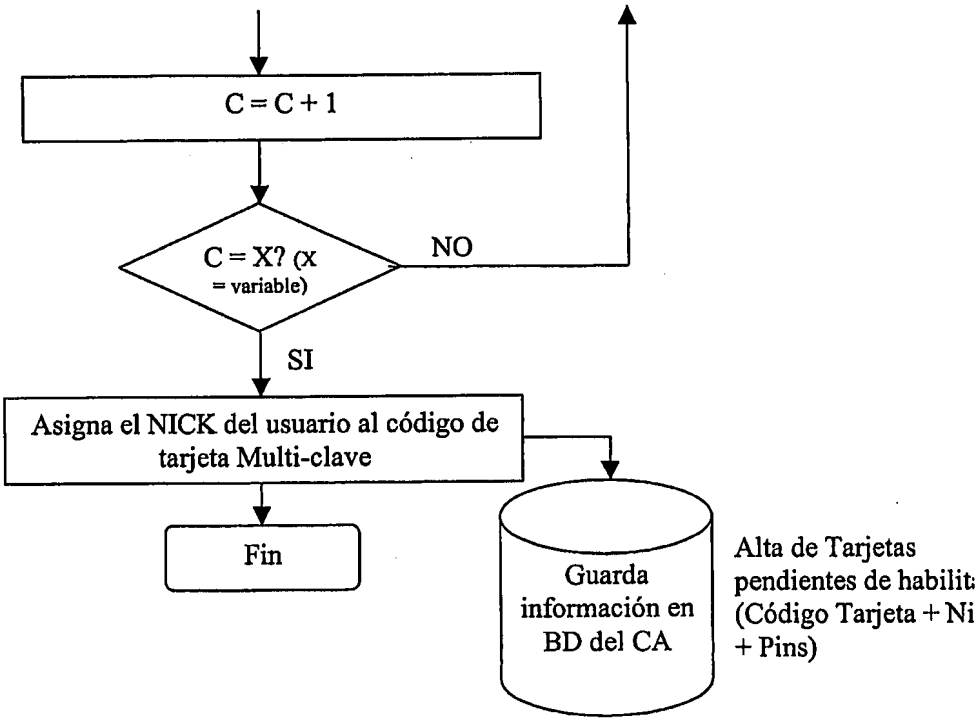
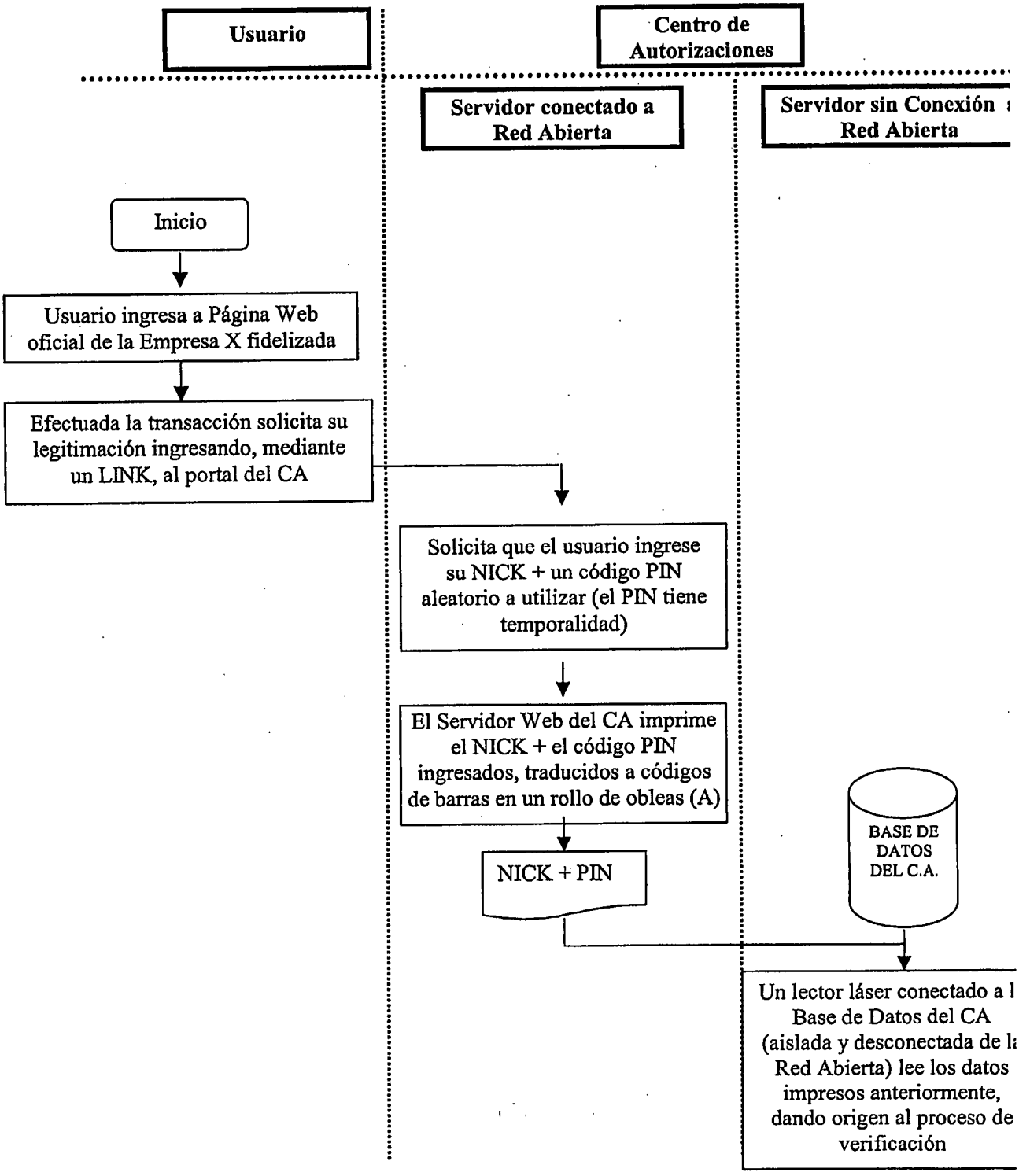


Figura 5



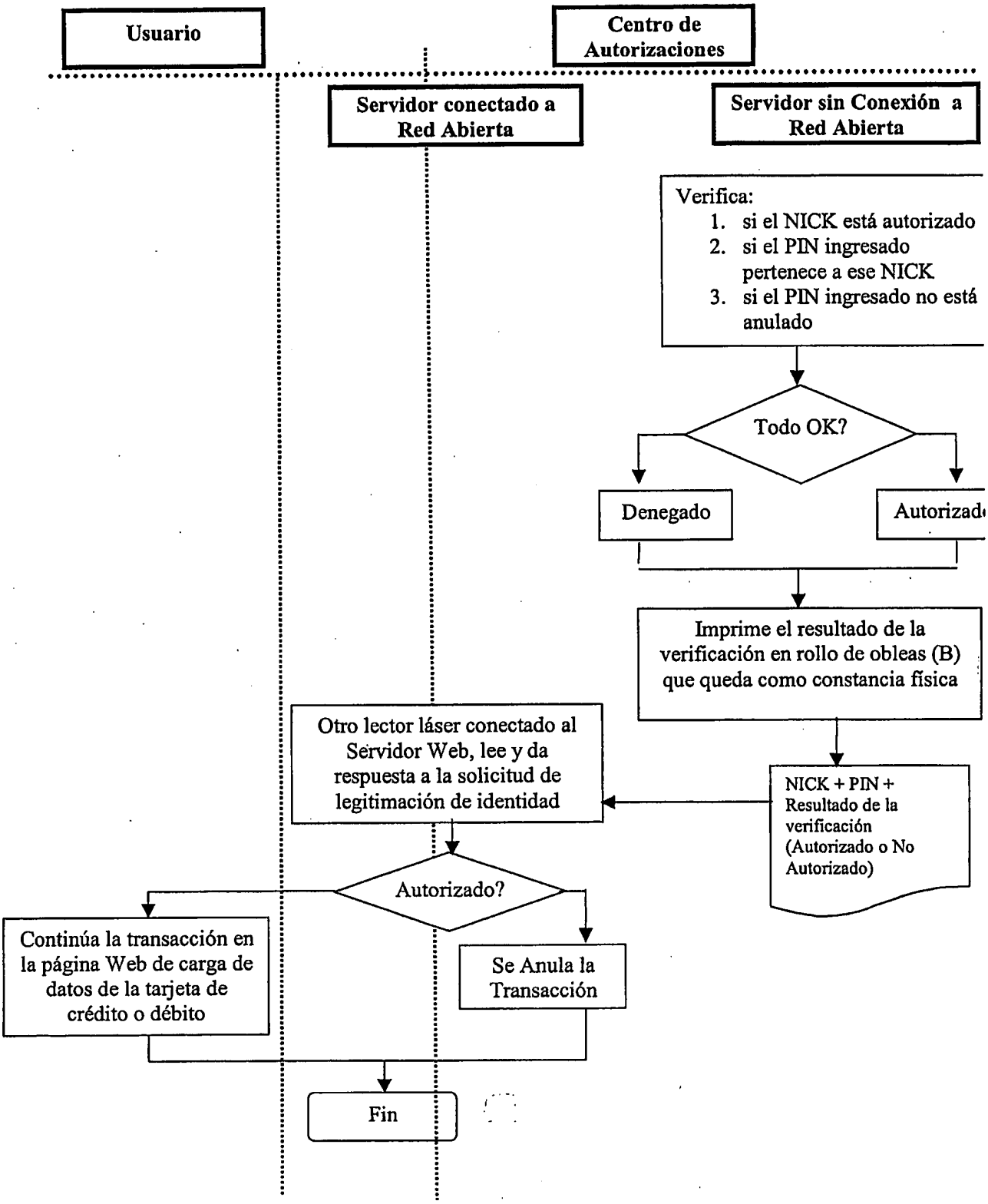

Usuario
Centro de Autorizaciones
Servidor conectado a Red Abierta
Servidor sin Conexión a Red Abierta
Verifica:
1. si el NICK está autorizado
2. si el PIN ingresado pertenece a ese NICK
3. si el PIN ingresado no está anulado
Todo OK?
Denegado
Autorizad
Imprime el resultado de la verificación en rollo de obleas (B) que queda como constancia física
NICK + PIN + Resultado de la verificación (Autorizado o No Autorizado)
Otro lector láser conectado al Servidor Web, lee y da respuesta a la solicitud de legitimación de identidad
Autorizado?
Continúa la transacción en la página Web de carga de datos de la tarjeta de crédito o débito
Se Anula la Transacción
Fin

Figura 6

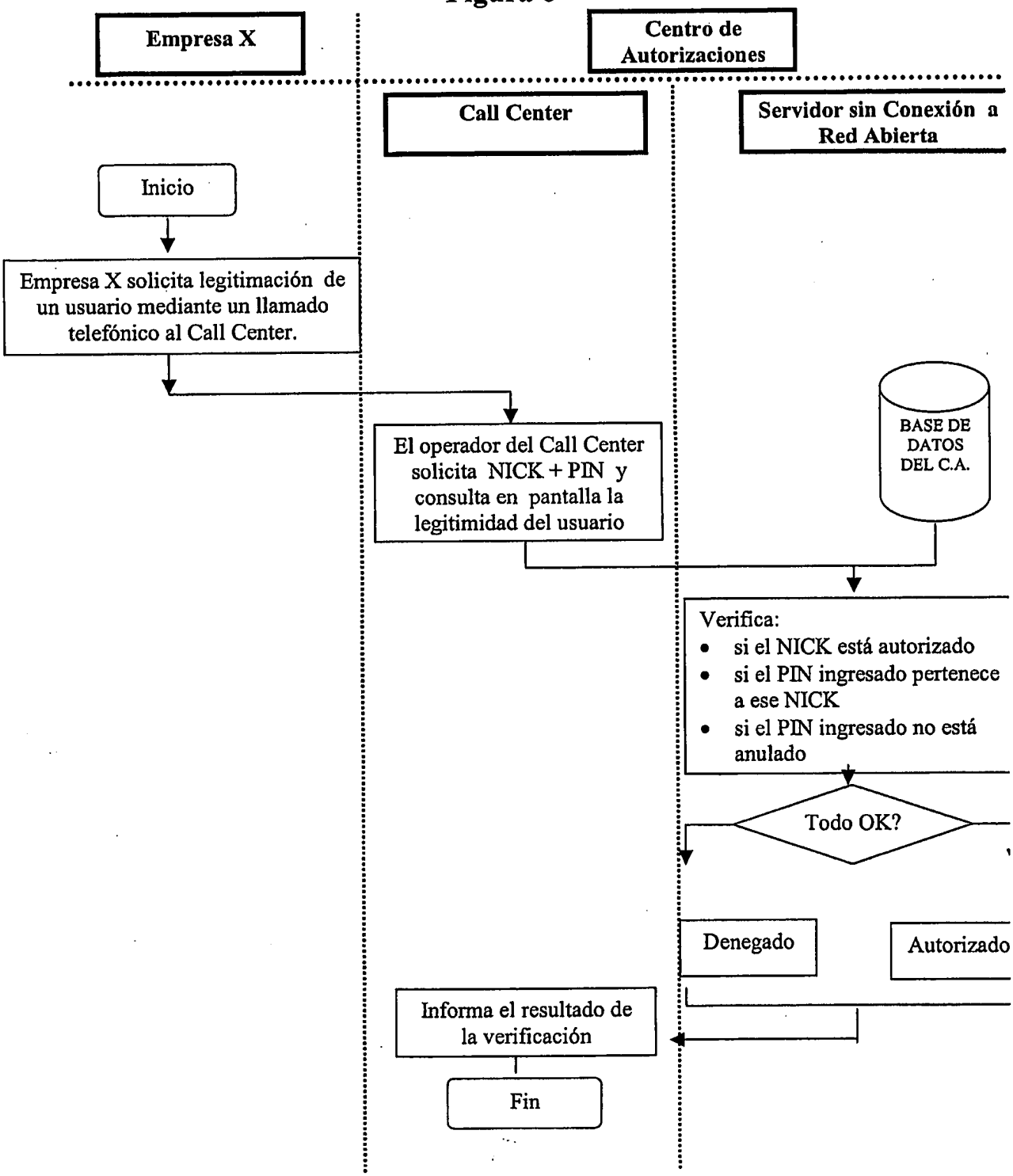
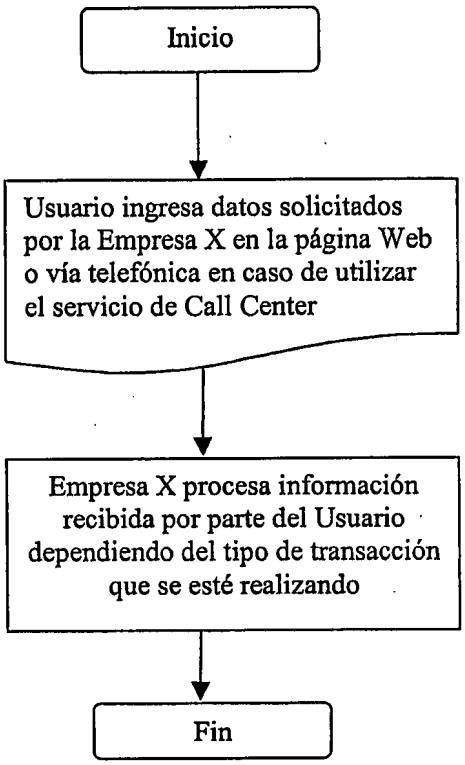

Empresa X
Centro de Autorizaciones
Call Center
Servidor sin Conexión a Red Abierta
Inicio
Empresa X solicita legitimación de un usuario mediante un llamado telefónico al Call Center.
El operador del Call Center solicita NICK + PIN y consulta en pantalla la legitimidad del usuario
BASE DE DATOS DEL C.A.
Verifica:
si el NICK está autorizado
si el PIN ingresado pertenece a ese NICK
si el PIN ingresado no está anulado
Todo OK?
Denegado
Autorizado
Informa el resultado de la verificación
Fin

Figura 7



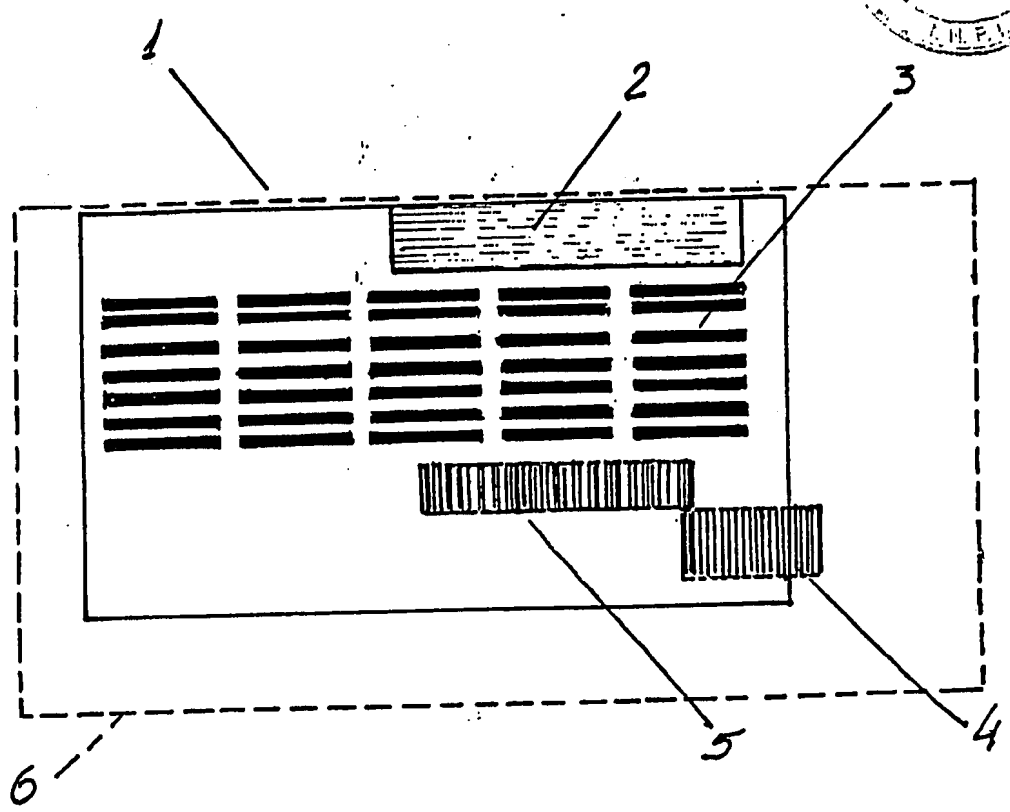


FIG.8